

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

TITLE

**AN IMPROVED TELEPHONY SECURITY SYSTEM**

INVENTORS

**DAVID L. BUNTIN**

**KEITH S. PICKENS**

**CERTIFICATE OF MAILING 37 C.F.R. § 1.10**

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as Express Mail, Express Mail No. EV 025739217 US, addressed to: Mail Stop Patent Application/Fee, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450; on February 13, 2004.

Venisa J. Dark

Name of Person Filing or Mailing Document

Venisa J. Dark

Signature of Person Mailing or Filing Document

**AN IMPROVED TELEPHONY SECURITY SYSTEM**

**Reference to Related Application**

[0001] This application is a continuation-in-part of U.S. Patent Application Serial  
5 No. 09/907,089 entitled TELEPHONY SECURITY SYSTEM filed July 17, 2001, which  
is a continuation-in-part of U.S. Patent No. 6,542,592B1 entitled TELEPHONY  
SECURITY SYSTEM filed October 19, 2001, which is a continuation of U.S. Patent No.  
6,320,948 B1 entitled TELEPHONY SECURITY SYSTEM filed June 14, 2000, which is  
a continuation of U.S. Patent No. 6,249,575 B1 entitled TELEPHONY SECURITY  
10 SYSTEM filed December 11, 1998, each assigned to the assignee of the present  
application. This application is also a continuation-in-part of U.S. Patent Application No.  
09/709,592, filed November 10, 2000, entitled "A System and Method for Encapsulation,  
Compression and Encryption of PCM Data", U.S. Patent Application No. 10/200,969,  
filed July 23, 2002, entitled "Encapsulation, Compression and Encryption of PCM Data",  
15 U.S. Patent No. 10/625,311, filed July 23, 2003, entitled "An Improved Virtual Private  
Switched Telecommunications Network", and U.S. Patent Application No. 10/649,204,  
filed August 27, 2003, entitled "An Improved Virtual Private Switched  
Telecommunications Network", all assigned to the assignee of the present invention and  
incorporated herein by reference.

20 [0002] This application claims the benefit of Provisional U.S. Patent Application  
60/488,232 filed February 16, 2003.

**Technical Field**

[0003] The invention relates generally to telecommunications monitoring and/or  
control systems and particularly to a telephony resource and security management system

for monitoring and/or controlling access between end-user stations and the public circuit-switched network and/or the public packet-switched network..

### **Background**

[0004] Currently, there are telecommunication firewalls that operate on  
5 traditional circuit-switched networks, implementing a centrally managed, policy-based, enterprise-wide security policy, performing designated actions (such as allowing or denying the call, recording the call, redirecting the call, and monitoring the call for keywords), based on the determined attributes of a circuit-switched call (such as call direction, call source, call destination, and call type). U.S. Patent Application Serial No.  
10 09/907,089 entitled TELEPHONY SECURITY SYSTEM describes a telecommunication firewalls that operates on traditional circuit-switched networks.

[0005] Unfortunately, there is no equivalent device for performing the same and similar tasks for VoIP (Voice over Internet Protocol) calls. Current IP firewalls are in place on the packet-switched network, but they deal with attributes of individual packets,  
15 not attributes of the real-time packet-switched call itself. This is indeed unfortunate because a majority of the same call attributes determined on a circuit-switched call can also be determined on a real-time packet-switched call.

[0006] Therefore, there is a need for a telephony security system and method that provides centrally managed, policy-based, enterprise-wide monitoring and/or control of  
20 incoming and outgoing real-time packet-switched calls between an enterprise's end-user station and the public packet-switched network, based on attributes of the call itself.

[0007] Additionally, there is a need for a telephony security system and method that provides consolidated, central, policy-based, enterprise-wide monitoring and/or control of calls on both a circuit-switched network and a packet-switched network

### SUMMARY

5 [0008] The present invention, accordingly, provides a system and method for centrally managed, policy-based, enterprise-wide enforcement of a security policy that designates monitoring and/or control functions to be performed on incoming and outgoing calls between an enterprise's end-user stations and two disparate networks—the public circuit-switched network and/or the public packet-switched network. In the most  
10 basic configuration, one or more rules are configured which designate at least one action to be performed based on at least one determined attribute of the inbound or outbound call.

[0009] The system determines specific attributes associated with inbound and outbound calls on circuit-switched and/or packet-switched networks. The system further  
15 determines, according to the rule whose criteria is matched by the determined attributes, whether certain inbound and outbound calls are allowed or denied, content-monitored for keywords, recorded, redirected, authorized for remote access, monitored for the presence of patterns of interest, conducted in encrypted mode. The rule-set may also designate that the system log the call event, adjust the security policy, sound a message or tone, generate  
20 real-time alerts, and generate reports. Alerts include, as examples: electronic mail notification, pager notification, console messaging, and/or a Simple Network Management Protocol (SNMP) trap notification.

[0010] Call attributes determined by the system include, as examples: call direction, call source, call destination, call-type (i.e., voice, fax, modem, STU-III-voice, STU-III-data, STU-III unspecified, Wideband data, Wideband video, IP telephone, busy, unanswered, and undetermined), call content such as keywords detected via speech  
5 recognition, or demodulated and decoded modem and/or fax data, call time, call date, call duration, the codec used, the number of bytes from the call source, the number of bytes from the call destination, the number of packets from the call source, the number of packets from the call destination, source and destination transmission rates; latency, jitter, packet loss, and total bandwidth used.

10 [0011] For all locations within the enterprise having telephony resources that are routed through a specialized in-line device (line sensor), the system monitors and/or controls access to telephone stations, fax machines, modems, STU-III devices, and video teleconference (VTC) stations on the enterprise private circuit-switched network, as well as access to IP telephones, and other elements on the enterprises private packet-switched  
15 network, including media gateways, call servers, IP firewalls, etc.

[0012] The present invention combines call-progress monitoring, caller-id (CND) and/or automatic number identification (ANI) decoding, digital line protocol reception, decoding, demodulation, pulse dial detection, tone detection (DTMF and MF), and speech recognition with microprocessor control, access-control logic, and call-interrupt circuitry  
20 for inspecting and analyzing circuit-switched calls and implementing the access control functions designated in the security policy.

[0013] Additionally, the present invention combines protocol decoding, decryption, and encryption, protocol translation/conversion, media packet decoding,

decryption, demodulation, tone detection, speech recognition, software virus/worm detection, network address translation, and media packet encryption with microprocessor control for inspecting and analyzing packet-switched calls and implementing the access control functions designated in the security policy.

5           [0014] As used herein, the following terms carry the connotations described below:

          [0015] “Public circuit-switched network” is understood to refer to a network for provision of circuit-switched circuits to the public, wherein a physical circuit is temporarily established on demand and kept reserved for the user until the network  
10 receives a disconnect signal.

          [0016] “Public packet-switched network” is understood to refer to a network for provision of packet-switched circuits to the public, wherein data is carried in the form of packets.

          [0017] “Keyword” is understood to refer to a predefined sequence of digital data.

15           [0018] “STU-III-voice” call-type is understood to refer to the encrypted voice transmission from a Secure Telephone Unit-III (STU-III) encryption device used by some government agencies, the military and some NATO agencies to conduct classified conversations.

          [0019] “STU-III-data” call-type is understood to refer to the encrypted data  
20 transmission from the STU-III encryption device when it is used as a modem to transmit data to another STU-III location.

[0020] “STU-III-unspecified” call-type is understood to refer to transmissions from the STU-III devices, but due to the early version of the device, a determination of STU-III-voice or STU-III-data can not be made.

[0021] “Wideband” call-type is understood to refer to any non-voice grade data transmission using multiple channels on an Integrated Services Digital Network/Primary Rate Interface (ISDN/PRI) trunk (except video which is referenced separately; i.e., the bearer channel information transfer capability attribute is “speech,” “3.1 kHz audio,” “restricted data,” “unrestricted data,” or “unrestricted data with tones/announcements”).

[0022] “Wideband video” call-type is understood to refer to any video transmission using multiple channels on a ISDN/PRI trunk (i.e., the bearer channel information transfer capability attribute is “video”).

[0023] “Unanswered” call-type is understood to refer to the call wherein the call source hangs up before the call destination answers.

[0024] “Undetermined” call-type is understood to refer to the call wherein the called or calling party hangs up after the call is answered but before the call-type is determined.

#### **BRIEF DESCRIPTION OF THE DRAWING FIGURES**

[0025] A better understanding of the system and method for monitoring and/or controlling incoming and outgoing circuit-switched and/or packet-switched calls between a public network and end-user stations located within an enterprise may be had by reference to the drawing figures wherein:

Figure 1A is a schematic block diagram illustrating one embodiment of a telephony security system of the present invention wherein circuit-switched calls are routed through the system at a line sensor located on an enterprise private circuit-switched network;

5        Figure 1B is a schematic block diagram illustrating an alternate embodiment of the system of Figure 1A wherein circuit-switched calls to/from an enterprise are routed through the system at a line sensor located on a public circuit-switched network;

Figure 1C is a schematic block diagram illustrating an alternate embodiment of the system of Figure 1A wherein real-time packet-switched calls are routed through the  
10        system at a line sensor located on the packet-switched network-side of a media gateway;

Figure 1D is a schematic block diagram illustrating an alternate embodiment of the system of Figure 1A wherein packet-switched calls are routed through the system at a line sensor connected parallel with an IP firewall;

Figure 1E is a schematic block diagram illustrating an alternate embodiment of the  
15        system of Figure 1A wherein packet-switched calls are routed through the system at a line sensor located on the public packet-switched network-side of an IP firewall;

Figure 1F is a schematic block diagram illustrating an alternate embodiment of the system of Figure 1A wherein packet-switched calls are routed through the system at a line sensor located on the private packet-switched network-side of an IP firewall;

20        Figure 1G is a schematic block diagram illustrating an alternate embodiment of the system of Figure 1A wherein packet-switched calls are routed through the system at a line sensor which is interconnected with an IP firewall;



Figure 1H is a schematic block diagram illustrating an alternate embodiment of the system of Figure 1A wherein packet-switched calls to/from an enterprise are routed through the system at a line sensor located on a public packet-switched network;

Figure 1J is a schematic block diagram illustrating an alternate embodiment of the system of Figure 1A wherein both circuit-switched and real-time packet-switched calls are routed through the system at line sensors located on the private circuit-switched network and on the packet-switched network-side of a media gateway;

Figure 1K is a schematic block diagram illustrating the preferred embodiment of the system of Figure 1A wherein both circuit-switched and packet-switched calls are routed through the system at a line sensor located on the private circuit-switched network and on the private packet-switched network;

Figure 1L is a schematic block diagram illustrating an alternate embodiment of the system of Figure 1A wherein both circuit-switched and packet-switched calls to/from an enterprise are routed through the system at a line sensor located on the public circuit-switched network and on the public packet-switched network;

Figure 2 is a functional block diagram illustrating a simplified example security policy and corresponding actions and features for use by the system of Figures 1A-1L;

Figure 3 is a functional block diagram illustrating simplified example security policy elements and interactions of a simplified example security policy for use by the system of Figures 1A-1L; and

Figures 4A, 4B, and 4C are a process flow diagram illustrating installation, configuration and operational processes of the system of Figures 1A-1L.

## **DESCRIPTION OF THE EMBODIMENTS**

[0026] Figures 1A-1L illustrate various configurations of a telephony security system 10 of the present invention, wherein incoming and outgoing calls between a public network and end-user stations within an enterprise are routed through the system 10 for monitoring and/or control of the calls pursuant to a security policy 202 (Figure 2). The public network may be made up of: (1) a public circuit-switched network 12; (2) a public packet-switched network 14; or (3) both the public circuit-switched network 12 and the public packet-switched network 14. The end-user stations may be made up of: (1) one or more end-user stations 16 located on an enterprise private circuit-switched network; (2) one or more end-user stations 18 located on an enterprise private packet-switched network; or (3) both the end-user stations 16 and the end-user stations 18.

[0027] For each embodiment described herein, the system 10 consists primarily of: (1) at least one specialized device (i.e., line sensor, appliance, telephony appliance) 20 installed in-line on a circuit-switched and/or a packet-switched network; and (2) one or more network-accessible computers and processors and one or more clients (either local or remote to the computers and processors), herein referred to singly as a remote management server 22. The remote management server 22 is connected to the line sensor 20 by a LAN, WAN, or Internet 24). Calls to/from the public circuit-switched network 12 and/or the public packet-switched network 14 are routed through the system 10 at the line sensor 20. The line sensor 20 includes means for determining one or more attributes of circuit-switched and packet-switched calls. The system 10 includes means for performing one or more actions pursuant to the security policy 202, wherein actions may be performed by the line sensor 20 and the remote management server 22. The system 10

may be located within the enterprise, or some or all of the components of system 10 may be located outside the enterprise.

[0028] Although not shown, a single line sensor 20 may be connected on both the circuit-switched network and/or the packet-switched network. It is understood that the line sensor 20 is not required at all of the connections and locations discussed below with reference to Figures 1A-1L. Rather, the line sensor 20 may be located in accordance with the configuration of lines and cabling, and in accordance with the enterprise's desired level of security and resource management.

[0029] Figure 1A illustrates one embodiment of the present invention wherein circuit-switched calls to/from the private circuit-switched network are routed through the system 10 at one or more line sensors 20 located on the private circuit-switched network, represented by a line sensor 20A, 20B, 20C and 20D. Station extensions 26 connect end-user stations 16 to either a Public Branch eXchange (PBX) 28 or a central office (not shown, located in the public circuit-switched network 12). The end-user stations 16 include as examples: a telephone 30; a fax machine 32; a modem 34; a STU-III device 36; and a Video TeleConference (VTC) station 38. The modem 34 may support, for example, desktop or portable personal computers, or systems requiring modems for remote dial-up monitoring or maintenance access, such as PBXs, routers, Heating, Ventilation and Air Conditioning (HVAC) systems, and alarm systems.

[0030] Connectivity of the line sensor 20 within the private circuit-switched network may be any combination of: (1) a PBX end-user station-side connection, represented by the line sensor 20A; (2) a PBX trunk-side connection, represented by the line sensor 20B; (3) a connection on a line directly connecting with a central office

located within the public circuit-switched network 12, represented by the line sensor 20C;  
and (4) a media gateway circuit-switched network-side connection, represented by line  
sensor 20D.

[0031] The remote management server 22 provides the primary user interface  
5 whereupon the system administrator programs the security policy 202 and other  
operational features of the system 10. The system administrator downloads the security  
policy 202 and other appropriate programming to all or selected line sensor 20 from the  
remote management server 22. The remote management server 22 receives call log event  
records from the line sensor 20 and performs tracking functions pursuant to the security  
10 policy 202. The remote management server 22 provides audio play-back of recorded  
voice call content; viewing and printing of reconstructed data call content; and  
consolidation, management, display and printing of call logs 204 and reports 206 (Figure  
2). Archiving of call logs 204, reports 206, and recorded and reconstructed call content  
may also be accomplished on the remote management server 22, or on another network-  
15 accessible server. The line sensor 20 and management server 22 may communicate  
within the enterprise network with various host computers for providing the reporting  
functions.

[0032] The remote management server 22 allows the system administrator to  
monitor system operations and view ongoing call activity and call logs 204 (including  
20 changes in call attributes) flowing through the line sensor 20, regardless of whether the  
line sensor 20 is located nearby or at a very remote distance therefrom.

[0033] The system administrator may preempt or complement actions the line  
sensor 20 performs in enforcing the security policy 202, thereby manually allowing or

denying a call, and/or causing the call to be redirected, recorded, content-monitored, authenticated for remote access, and/or conducted in encrypted mode. The system administrator may preempt or complement line sensor 20 actions from either the remote management server 22, client, or the specific line sensor 20 whose actions are to be preempted or complemented.

[0034] The remote management server 22 detects a loss of power to, operation of, or communication with the line sensor 20. Upon detection of such an event, the remote management server 22 logs the event, generates a report and/or alert to designated personnel, pursuant to the security policy 202. If the connection between the remote management server 22 and the line sensor 20 is lost, the line sensor 20 continues to enforce the security policy 202. Policies also remain in effect if the line sensor 20 reboots. Additionally, if a loss of service on the line or cabling is detected, the remote management server 22 performs administrator-designated logging, reporting, and alert notifications.

[0035] Referring again to the connection represented by line sensor 20D, a LAN or WAN (LAN/WAN) 42 connects end-user stations 18 to components on the private packet-switched network 40, including a media gateway 44. The end-user stations 18 include an example: an IP telephone 46. Routing all real-time packet-switched (VoIP) calls through the line sensor 20D, located on the circuit-switched network-side of the media gateway 44, allows the system 10 to monitor and/or control real-time packet-switched calls from end-user stations 18 on the private packet-switched network.

[0036] Figure 1B illustrates an alternate embodiment of the present invention wherein circuit-switched calls to/from an enterprise are routed through the system 10 at

one or more line sensors 20 located on the public circuit-switched network 12, represented by a line sensor 20E. This embodiment allows service providers to offer centralized monitoring and/or control of circuit-switched calls between the public circuit-switched network 12 and the customer private circuit-switched network, pursuant to the security policy 202 configured to meet the needs of the customer enterprise.

[0037] Connectivity of the system 10 within the public circuit-switched network 12 may be any combination of: (1) a connection on a line directly connecting end-user stations with the central office (CO) (similar to that represented by line sensor 20C), with the line sensor 20E connected outside the perimeter of the customer private circuit-switched network; (2) a CO trunk-side connection, between the CO and the perimeter of the customer private circuit-switched network; (3) a connection within the CO; and (4) a connection in the public circuit-switched network wherein the line sensor 20E is in an auxiliary position and the carrier purposefully routes traffic to and from the line sensor 20E; each represented by the line sensor 20E.

[0038] The remote management server 22 may be located: (1) outside the customer enterprise; (2) within the customer enterprise; or (3) outside the customer enterprise with one or more remote clients located within the customer enterprise to provide the customer's administrators with access to all or some of the operational features of the remote management server 22.

[0039] Figure 1C illustrates an alternate embodiment of the present invention wherein real-time packet-switched calls are routed through the system 10 at one or more line sensors 20 located on the packet-switched network-side of the media gateway 44, represented by a line sensor 20F. The LAN/WAN 42 connects the end-user stations 18 to

components on the private packet-switched network 40, including the media gateway 44, a call manager (call server) 54, and an IP firewall 56. All packet-switched traffic that is not real-time traffic (e.g., http, electronic mail, etc.), is routed through and processed by the IP firewall 56. All real-time packet-switched traffic is routed through the line sensor 20F, which processes the real-time packets pursuant to the security policy 202.

[0040] The line sensors 20 may also be located at points of converging and concentrated network signaling (e.g., at network elements such as the call server 54, proxy servers, IP PBXs, etc.), as represented by line sensor 20G, located between the call server 54 and the end-user stations 18.

[0041] Figure 1D illustrates an alternate embodiment of the present invention wherein packet-switched calls are routed through the system 10 at one or more line sensors 20 parallel with the IP firewall 56, represented by a line sensor 20H. The traffic that is not real-time packet-switched traffic is routed through and processed by the IP firewall 56. Real-time packet-switched traffic is routed through the line sensor 20H, which processes the real-time packets pursuant to the security policy 202.

[0042] Alternatively, all packet-switched traffic may be routed through both the line sensor 20H and the IP firewall 56. In this embodiment, the line sensor 20H processes the real-time packets pursuant to the security policy 202 and discards packets that are not real-time packets. The IP firewall 56 processes packet-switched traffic that is not real-time traffic and discards the real-time packet-switched traffic. .

[0043] Figure 1E illustrates an alternate embodiment of the present invention wherein real-time packet-switched calls are routed through the system 10 at one or more line sensors 20 located on the public packet-switched network-side of the IP firewall 56,

represented by a line sensor 20J. The IP firewall 56 processes all traffic that is not real-time packet-switched traffic and passes on, untouched, all real-time packet-switched traffic. The line sensor 20K processes all real-time packets pursuant to the security policy 202 and passes on, untouched, all traffic that is not real-time packet-switched traffic.

5           [0044] Figure 1F illustrates an alternate embodiment of the present invention wherein real-time packet-switched calls are routed through the system 10 at one or more line sensors 20 located on the private packet-switched network-side of the IP firewall 56, represented by a line sensor 20K. The IP firewall 56 processes all traffic that is not real-time packet-switched traffic and passes on, untouched, all real-time packet-switched  
10 traffic. The line sensor 20K processes the real-time packets pursuant to the security policy 202 and passes on, untouched, all traffic that is not real-time packet-switched traffic.

          [0045] Figure 1G illustrates an alternate embodiment of the present invention wherein real-time packet-switched calls are routed through the system 10 at one or more  
15 line sensors 20 interconnected with the IP firewall 56, represented by a line sensor 20L. The IP firewall 56 processes all traffic that is not real-time packet-switched traffic and sends all real-time packet-switched traffic to the line sensor 20M for processing. The line sensor 20M processes the real-time packets pursuant to the security policy 202 and sends processed packets back to the IP firewall 56 for forwarding.

20           [0046] Figure 1H illustrates an alternate embodiment of the present invention wherein packet-switched calls to/from an enterprise are routed through the system 10 at one or more line sensors 20 located on the public packet-switched network 14, represented by a line sensor 20M. This embodiment allows service providers to offer



centralized monitoring and/or control of real-time packet-switched calls between the public packet-switched network 14 and components (e.g., end-user stations 18) on the customer private packet-switched network 40, pursuant to the security policy 202. The line sensor 20M processes the real-time packets pursuant to the security policy 202 and  
5 passes on, untouched, all traffic that is not real-time packet-switched traffic. Components on the customer private packet-switched network 40 (e.g., the IP firewall 56) process the packet-switched traffic that is not real-time traffic.

[0047] Connectivity of the system 10 within the public packet-switched network 14 may be any combination of: (1) a connection on a line directly connecting end-user  
10 stations with the service provider's central office facility, with the connection located outside the perimeter of the customer private packet-switched network; (2) a service provider's central office facility trunk-side connection, between the service provider's central office facility and the perimeter of the customer private packet-switched network; (3) a connection within the service provider's central office facility; and (4) a connection  
15 in the public packet-switched network wherein the line sensor 20M is in an auxiliary position and the carrier purposefully routes traffic to and from the line sensor 20M; each represented by the line sensor 20M.

[0048] The remote management server 22 may be located: (1) outside the customer enterprise; (2) within the customer enterprise; or (3) outside the customer  
20 enterprise with one or more remote clients located within the customer enterprise to provide the customer's administrators with access to all or some of the operational features of the remote management server 22.

[0049] Figure 1J illustrates an alternate embodiment of the present invention wherein both circuit-switched and real-time packet-switched calls are routed through the system 10 at one or more line sensors 20 connected on the private circuit-switched network and on the packet-switched network-side of the media gateway 44. Circuit-switched calls are routed through the line sensor 20A, 20B, and 20C, as described with reference to Figure 1A. Real-time packet-switched traffic is routed through the line sensor 20F, as described with reference to Figure 1C. This embodiment provides centralized monitoring and/or control of both circuit-switched calls to/from the private circuit-switched network and real-time packet-switched calls to/from the private packet-switched network 40.

[0050] Figure 1K illustrates the preferred embodiment of the present invention, wherein both circuit-switched and packet-switched calls are routed through the system at one or more line sensors 20 connected on both the private circuit-switched network and on the private packet-switched network 40 parallel with the IP firewall 56. This embodiment provides centralized monitoring and/or control of calls to/from both the private circuit-switched network and the private packet-switched network 40. Circuit-switched calls are routed through the line sensor 20A, 20B, and 20C, as described with reference to Figure 1A. Packet-switched traffic is routed through the line sensor 20H, as described with reference to Figure 1D. This embodiment provides centralized monitoring and/or control of calls to/from both the private circuit-switched network and the private packet-switched network 40.

[0051] Although not shown, alternate embodiments are contemplated wherein circuit-switched calls are routed through the system 10 at line sensor 20A, 20B, and 20C, as described with reference to Figure 1A, and packet-switched traffic is routed through

the system 10 at line sensor 20J, 20K, or 20L as described with reference to Figure 1E, 1F, or 1G, respectively.

[0052] Figure 1L illustrates an alternate embodiment of the present invention wherein circuit-switched calls are routed through the system 10 at line sensor 20E, as described with reference to Figure 1B, and packet-switched calls are routed through the system 10 at line sensor 20M, as described with reference to Figure 1H. This embodiment allows service providers to offer centralized monitoring and/or control of both circuit-switched calls between the public circuit-switched network 12 and the customer private circuit-switched network, and real-time packet-switched calls between the public packet-switched network 14 and components (e.g., end-user stations 18) on the customer private packet-switched network 40, pursuant to a security policy 202.

[0053] It is understood that one or more lines, trunks, and/or cabling may be mapped through any single line sensor 20 (e.g., line sensor 20A and 20B show connectivity with multiple circuit-switched lines). Although not shown, any single line sensor 20 may be connected on both the circuit-switched network and/or the packet-switched network, the line sensor 20 being located in accordance with the configuration of lines and cabling, and in accordance with the enterprise's desired level of security and resource management. Accordingly, the security policy 202 that is downloaded to the line sensor 20 may be configured to address both circuit-switched and/or packet-switched calls.

[0054] As represented by the line sensor 20A–20M and its corresponding line(s), it is understood that the line sensor 20 is configured to map the station extensions, direct connect lines, trunks, and/or cabling through the line sensor 20. The system 10 is

transparent to the end-user stations 16 and 18, the central office, the PBX 28, the media gateway 44, the call server 54, and the IP firewall 56, unless the security policy 202 designates authentication of remote access or termination of a call (i.e., all lines and cabling terminate at the same points as prior to installation of the line sensor 20, call traffic is uninterrupted if power is removed from the line sensor 20, call traffic is uninterrupted if a call is in progress when the line sensor 20 comes on-line, and the call content received by the destination is identical to the call content transmitted by the source).

[0055] Referring to Figure 2, a functional schematic 200 illustrates certain operational aspects of the system 10. An example (very simplified) security policy 202 is shown for monitoring and/or controlling the flow of calls through the line sensor 20. As exemplified in Figure 2 and discussed below and in further detail later with reference to Figure 3 and 4, the security policy 202 is administrator-configured, and implements a rule-set designating at least one action to be performed based upon at least one attribute of an incoming and/or outgoing call. It is understood that the rule-set is implemented by software instructions within the line sensor 20 and remote management server 22 that may be programmed or modified at either the line sensor 20 or at the remote management server 22 located nearby or at a very remote distance therefrom. It is further understood that since any single line sensor 20 may be connected on both the circuit-switched network and the packet-switched network, the security policy 202 that is downloaded to the line sensor 20 may be configured to address both circuit-switched and packet-switched calls.

[0056] A call log 204 is constructed for each call, consisting of concatenated call event records, and stored in a database on the remote management server 22. Real-time

ongoing and historical call log(s) 204 are viewed and printed from the remote management server 22. Although the call log 204 shown in Figure 2 is a very simplified example, the administrator-designated level of detail of the call log 204 ranges from verbose (including all call attributes, all call events, and all actions and tracking functions performed), to very brief (including only selected call attributes, call events, actions and tracking functions).

[0057] The call log 204 details, attributes determined by the line sensor 20, and security policy 202 rule criteria that are common to both monitoring and/or controlling calls on circuit-switched and packet-switched networks includes one or more of the following:

Call Key - a unique identifying key assigned to each call by the line sensor 20;

Line sensor Name - the designated alias of the line sensor 20 processing the call and enforcing the rule;

Line sensor Group - the designated alias of the group (or array of line sensors 20) to which the line sensor 20 processing the call belongs;

Start Date - the start date of the call;

Start Time - the start time of the call;

Direction - whether the call is inbound or outbound;

Raw Destination Information – the digits dialed or information preceding call connection, including prefix, the base destination phone number or information, suffix, etc.;

Source – extension assigned to the end-user station 16 for outbound calls, number extracted from Caller ID (or other means) for inbound calls, mask, IP address, IP subnet (IP address and netmask), port, user agent, user identifier (e.g., john.doe@company.com), uniform resource identifier (URI), domain, etc. where the source is  
5 initiating the call;

Source Name –alias of the source initiating the call;

Destination – extension assigned to the end-user station 16 for outbound calls, number extracted from Caller ID (or other means) for inbound calls, mask, IP address, IP subnet (IP address and netmask), port, user agent, user identifier (e.g., john.doe@  
10 company.com), uniform resource identifier (URI), domain, etc. where the destination is receiving the call;

Destination Name – alias of the destination receiving the call;

Connect Time – the time at which the call was answered (connected);

Security Policy – the designated alias of the security policy 202 containing the  
15 matched (fired) rule;

Rule Number. – the number of the rule that matched the determined call attributes and therefore fired;

Call-Type - the type of call/payload (e.g., voice, fax, modem, voice energy, modem energy, STU-III-data, STU-III-voice, STU-III-unspecified, wideband data,  
20 wideband video, video, IP voice, FNBBDT, TTY/TDD, busy, unanswered, undetermined, etc.);

Call Content – designated keyword (predefined sequence of digital data) detected in calls via speech recognition or demodulated modem and/or fax data;

Actions – designated actions executed by the line sensor 20, pursuant to the security policy (i.e., allowing or denying the call);

5 Tracks – additional actions and tracking functions executed, pursuant to the security policy 202 (e.g., line sensor 20 additional actions include: recording call content, redirecting the call, authenticating remote access, monitoring call content for keywords, conducting the call in encrypted mode; remote management server 22 tracking functions include: adjusting the security policy, logging call events, generating notification alerts  
10 and generating reports);

Redirect – the port and name of the peripheral device the call is redirected to;

Post-connect information – digits/information sent after the call is connected;

Log Time – the date and time a call event record is appended to the call log 204;

Call Log Comment – Comments included in the call log 204, for the benefit of the  
15 system administrator, which are associated with the fired rule and call event (e.g., unauthorized outbound modem; keyword detected in call content; call content recorded, bandwidth threshold exceeded, etc.);

End Date – the date the call ended;

End Time – the time the call ended; and

20 Duration – the duration of the call (in seconds).

[0058] The call log 204 details, attributes determined by the line sensor 20, and security policy 202 rule criteria that are common to both monitoring and/or controlling calls on circuit-switched networks includes one or more of the following:

Line - the identifier for the line (extension, direct connect, etc.) carrying the call;

5 Trunk - the PBX trunk through which the call is processed;

Channel - the channel through which the call is processed;

Prefix – all digits or information preceding the base destination, including outside access number, long distance access code, etc.; and

Suffix – all digits or information following the base destination, including DTMF-  
10 based Personal Identification Number (PIN) code used in authentication for remote access, calling card numbers, etc.

[0059] The call log 204 details, attributes determined by the line sensor 20, and security policy 202 rule criteria that are common to both monitoring and/or controlling calls on packet-switched networks includes one or more of the following:

15 Codec – method of audio signal encoding used for real-time packet-switched call (e.g., G.711, G.723, G.729, etc.);

Bytes from Source –number of bytes transferred from the source of the call;

Bytes from Destination –number of bytes transferred from the destination of the call;

20 Packets from Source – number of packets transferred from the source of the call;



Packets from Destination –number of packets transferred from the destination of the call;

Source Transmission Rate – the rate of packet traffic from the call source in bytes/second;

5 Destination Transmission Rate – the rate of packet traffic from the call destination in bytes/second;

Source Latency – period of delay (seconds or milliseconds) in the arrival of packets from the call source;

Destination Latency – period of delay (seconds or milliseconds) in the arrival of  
10 packets from the call destination;

Source Jitter – period of deviation in latency (milliseconds or microseconds) of packets from the call source;

Destination Jitter – period of deviation in latency (milliseconds or microseconds) of packets from the call destination;

15 Source Packet Loss -- difference between the number of expected packets (based on sequence numbers, headers, the number of packets seen for the same call at another point in the network, etc.) and the number of packets that actually arrived from the call source;

Destination Packet Loss – difference between the number of expected packets  
20 (based on sequence numbers, headers, the number of packets seen for the same call at

another point in the network, etc.) and the number of packets that actually arrived from the call destination;

Virus – a virus is in the media or signaling stream;

Anomalous call – unexpected expected call attribute or set of attributes given  
5 previous call history or user defined limits;

Malformed packet/message – a poorly formed message (i.e. too long, too short, incorrect fields, etc) in the signaling or media stream;

Signaling or media protocol version; and

Total Bandwidth – total number of bytes transferred from both the source and the  
10 destination.

[0060] It is further understood that the above listing is by no means exhaustive, and that any call attribute available on lines which carry a call, packet, or call information through the line sensor 20 may be used to configure rules, enforce the security policy 202, provide visibility, call activity logging, and reporting on inbound and outbound calls.

15 [0061] A recording module 205, located within the line sensor 20, records the raw binary stream of designated calls, pursuant to the security policy 202, and archives the data on the remote management server 22, located nearby or a great distance therefrom. The line sensor 20 temporarily caches the recorded content if the connection between the remote management server 22 and the line sensor 20 is lost. Several configurations are  
20 contemplated, including those whereby the functions of the recording module 205 are accomplished within the line sensor 20, within the remote management server 22, or

using a separate peripheral recorder 236 to which calls are redirected pursuant to the security policy 202.

[0062] Pursuant to the security policy 202, a VPN module 214, located within the line sensor 20, encrypts and transmits, receives and decrypts designated calls, thereby constructing a virtual private network (VPN) across the public circuit-switched network 12 or the public packet-switched network 14, between two line sensors 20, one located at each end of the call. If the security policy 202 designates that a call is to be conducted in encrypted mode, capabilities are negotiated between the two line sensors 20 and the call is conducted in encrypted mode without any action being taken by the called or calling parties to secure the call.

[0063] Encrypted transport of a call across the public circuit-switched network 14 and/or the public packet-switched network 16, from a first line sensor 20 location to a second line sensor 20 location, is implemented between one or more end-user stations located at the first enterprise location and one or more end-user stations located at the second enterprise location. The method includes the steps of: (1) defining at least one rule associated with the end-user stations at the first enterprise location, which designates the call is to be encrypted, based on at least one attribute of the incoming or outgoing call to/from the first enterprise location; (2) defining at least one rule associated with the end-user stations at the second enterprise location, which designates the call is to be encrypted, based on at least one attribute of the incoming or outgoing call to/from the second enterprise location; (3) determining the at least one attribute of the incoming or outgoing call to/from the first enterprise location; (4) determining the at least one attribute of the incoming or outgoing call to/from the second enterprise location; (5) performing the at least one action (encrypting the call) designated in the at least one rule associated

with the end-user stations at the first enterprise location; and (6) performing the at least one action (encrypting the call) designated in the at least one rule associated with the end-user stations at the second enterprise location.

[0064] It is contemplated that the system 10 may conduct a circuit-switched call  
5 in encrypted mode using one of several different methods, such as those described in greater detail in U.S. Patent Application No. 09/709,592, entitled "A System and Method for Encapsulation, Compression and Encryption of PCM Data;" U.S. Patent Application No. 10/200,969, entitled "Encapsulation, Compression and Encryption of PCM Data;" U.S. Patent Application No. 10/625,311, entitled "An Improved Virtual Private Switched  
10 Telecommunications Network;" and U.S. Patent Application No. 10/649,204, entitled "An Improved Virtual Private Switched Telecommunications Network;" all assigned to the assignee of the present invention and incorporated herein by reference. Similarly, two line sensors 20 conduct a call in encrypted mode on a packet-switched network using IPSEC and/or other security standards to encrypt the voice payload inside the packet,  
15 pursuant to the security policy 202. Capability negotiation, authentication and key management, is performed, although steps such as requesting a clear channel, synchronization, and compressing the payload, etc. are not necessary, as will be understood by those skilled in the art.

[0065] The report module within the remote management server 22 consolidates  
20 and manages designated call log 204 data for use in assessing an enterprise's resource usage and/or security posture. The numeral 206 represents at least one of a group of reports such as a post-event report 218, a schedule-generated report 220, or an ad hoc report 222, which may be initiated, or scheduled for later generation and delivery via a graphical user interface-based report module (not shown).

[0066] Reports are configuration-edited, generated, archived, displayed and printed via the remote management server 22. Report criteria includes: the date/time range for which call log data will be retrieved; call log 204 fields to be used; data organization (sorting, filtering, grouping, ordering); data presentation level (in detail or  
5 high level summary); and data display format (charts, graphs, or trends). It is understood that any configurable report, and any number of reports may be scheduled for generation and display, printing, or delivery at any discrete time or number of recurring time(s).

[0067] The post-event report 218 contains predefined information concerning a designated call event and is generated responsive to the call event, pursuant to the  
10 security policy 202.

[0068] The schedule-generated report 220 contains previously designated categories of call log data and is automatically generated, displayed, printed, and delivered at previously designated, discrete or recurring times and/or days. The schedule-generated report 220 is delivered to the designated recipient(s) by electronic mail  
15 message, to the designated file directory on a network– or web–accessible server, and/or to the designated archival file directory.

[0069] The ad hoc report 222 is manually initiated by authorized personnel. Both the schedule-generated report 220 and the ad hoc report 222 may include, for example, batch analysis of call log data for trending or difference/comparison reporting, either in  
20 great detail or high-level summary.

[0070] The remote management server 22 generates several types of alerts pursuant to the security policy 202, including, for example: electronic mail notification 224, pager alerting 226, console messaging (not shown), and SNMP trap notification (not

shown). Alert contents are administrator-configurable, derived from the call log 204 data, and may include, for example: rule number fired, call source, call destination, call type, line sensor 20 group and name, security policy name, designated keywords found in call content, date, and time.

5           [0071] The numeral 228 represents at least one of a group of peripheral devices to which the system 10 redirects the call or an in-progress copy of the call, pursuant to the security policy 202. The peripheral devices 228 may include, for example: a security listening station 230, a data Network Intrusion Detection System (NIDS) 234, and the recorder 236. While not shown, it is understood that the security policy 202 can also be  
10   configured such that any call to or from one or more designated end-user stations 16 and 18, source, or destination is redirected to a different end-user station 16 and 18 or destination. Several configurations are contemplated, including those whereby all functions and operations of the NIDS 234 are accomplished within the line sensor 20; or within the remote management server 22; or using a separate computer system(s), to  
15   which calls are redirected for analysis, any of which may be located nearby or a great distance therefrom.

          [0072] Figure 3 is a schematic block diagram of the exemplary security policy 202 for enforcement by the system 10. As described below, the security policy 202 is made up of one or more rules designating at least one action to be performed based on at  
20   least one attribute of the incoming or outgoing call between the public circuit-switched network and/or the public packet-switched network and the one or more end-user stations located within the enterprise's one or more locations.

[0073] The line sensor 20 compares the determined call attributes with the rules in the security policy 202, moving through the rule-set in sequential order, until either all criteria in a rule is met, or no rules meet the call attributes. It is understood that the security rule base 302 and result response policy 304 may include any number and types of rules, constructed using boolean combination (AND, OR, NOT) of any of the call attributes contained in the call log 204 and previously described with reference to Figure 2.

[0074] The rule-set is exited after any one rule matches the determined call attributes. Because call-type detection is continuous during the call, change in call-type during a call is detected. Consequently, each rule in the security policy 202, except for the rule already fired by the call's previous attribute, is re-evaluated in sequential order, using the updated call-type attributes. Actions and track functions are then performed based upon the rule matched with the updated call attribute. It is understood that the system 10 is capable of operating in a continuous processing loop, including detecting call attributes and analyzing call activity while simultaneously performing actions in accordance with the rules in the security policy 202. Any combination of action(s) or tracking function(s) may be included in the security rule base 302 and result response policy 304, pursuant to the enterprise's telephony security and resource management needs.

[0075] When designated in a rule, the following actions (and tracking functions) are performed by the line sensor 20:

allowing the call,

denying the call,

redirecting the call;

recording the call content,

encrypting the call,

sending a tone,

5 sending a message,

authenticating an inbound call for remote access, and

monitoring the call content for keywords.

[0076] When designated in a rule, the following actions (tracking functions) are performed by the remote management server 22:

10 logging the call,

generating a report,

generating an alert, and

adjusting the security policy.

[0077] Each rule includes the line sensor 20 location/identifier “install on,”  
15 allowing the system administrator to implement one security policy 202 containing rules to be applied to specific, designated line sensors 20.

[0078] As shown in Figure 2, the security policy 202 may include one or more security rule bases 302, one or more corresponding result response policies 304, and one or more groups 306 for a large globally distributed enterprise, however, for the sake of



clarity and simplicity, only one of each component is shown in this diagram. The one or more groups 306 may be for example: a keyword group 308, a codec group 312, and extension groups 314. Although shown schematically herein a more complex and detailed example of the security rule base 302 and result response policy 304 is discussed and illustrated in greater detail in U.S. Patent Application Serial No. 09/907,089 entitled TELEPHONY SECURITY SYSTEM.

[0079] The security rule base 302 is a sequential listing of rules, residing within the security policy 202 in the remote management server 22 and the line sensor 20. The security rule base 302 designates at least one action to be performed based on at least one determined attribute of the incoming or outgoing call. For example, a rule within the security rule base 302 might read "Allow inbound modem calls from any number in the maintenance dial-up group to any extension in the dial-up systems group, record call content, monitor call content for modem keywords, generate email, and log the event."

[0080] In the present example, the security rule base 302 designates: (1) record call content on a designated IP phone; (2) deny unknown or unauthorized modems; (3) record and monitor call content of all fax and modem calls; (4) record and monitor call content of all fax and modem calls, and calls on designated telephones and IP phones for designated keywords; (5) allow calls to/from IP phones, email if jitter exceeds designated threshold; (6) conduct any intra-enterprise voice call in encrypted mode.

[0081] The result response policy 304 is a sequential listing of response rules (similar in construction to the security rule base 302), which define the appropriate response to: call events; designated call attributes (e.g., the source's or destination's current group); the fired rule containing "adjust policy" as a track function (action); and a

result 330 of a threat assessment or an attempted action such conducting the call in encrypted mode. The result response policy 304 defines whether the call will be allowed or denied, or whether other actions will be performed, such as: playing a tone or message to the called/calling parties; generating an alert; generating a report, and automatically  
5 adjust the security policy (i.e., the remote management server 22 moves the designated source or destination from its current group to another different, designated group).

[0082] Threat assessments (TA) are actions performed by the line sensor 20 which include for example: authentication (via detection of dialed DTMF digits) of call sources attempting to remotely access enterprise telephony resources; monitoring the  
10 content of calls for designated keywords; monitoring calls for the presence of patterns of interest; and monitoring modem content for the presence of data of interest. The TA result 330 (i.e., the success or failure in authenticating the call source, identifying designated keywords, identifying patterns of interest, and/or data of interest), is used to identify an appropriate response to the assessment, pursuant to the result response policy  
15 304.

[0083] In Figure 2, the result response policy 304 designates: (1) adjust the security policy by moving the extension/IP address (i.e., identifier) of any modem call that is from/to an unauthorized source/destination into the unauthorized modem group; (2) adjust the security policy by moving the extension/IP address of any unknown or  
20 unauthorized modem into the unauthorized modem group on their first use; (3) adjust the security policy by moving the extension/IP address of any authorized modem call, found to contain designated keywords, into the modem content violation group; (4) adjust the security policy by moving the extension/IP address of any authorized fax call, found to contain designated keywords, into the fax content violation group; (5) adjust the security

policy by moving the extension/IP address into the voice content violation group, if the call content is found to contain designated keywords; (6) allow successfully encrypted calls between extension/IP address in the intra-enterprise group; allow calls between extension/IP address in the intra-enterprise group that failed to be encrypted, but sound a  
5 warning tone.

[0084] It is contemplated that the system 10 will make extensive use of groups 306 as a portion of the security policy 202. Objects such as sources, destinations, call types, keyword digital data sequences, codecs, PIN codes and extensions/IP addresses (i.e., identifiers) may be “bundled” together in logical groups 306 and collectively  
10 referred to by meaningful aliases for ease of management and convenience in applying rules (shown schematically herein as groups 308, 312, and 314 and discussed and illustrated in greater detail in U.S. Patent Application Serial No. 09/907,089 entitled TELEPHONY SECURITY SYSTEM). The keyword groups 308 is an example of grouping aliases for administrator-configured digital data sequences configured in  
15 keyword libraries to facilitate detection of keywords in call content that indicate improper behavior, security issues, or inappropriate use of telephony resources. It is understood that groups may overlap one another and even contain other groups entirely.

[0085] As shown in Figure 3, when the security rule base 302 or the result response policy 304 designate that the security policy is to be adjusted, the remote  
20 management server 22 removes an extension from its current extension group and places the extension into a different, designated extension group (e.g., removes an extension from the voice-only group 316 and places it in the unauthorized modem group 322), thereby altering the way in which the system 10 monitors and/or controls future calls to and from the moved extension.

[0086] Figures 4A, 4B, and 4C together show a process flow diagram 400 illustrating installation, configuration and operation processes for the system 10. Once installed and configured, it is understood that the system 10 is capable of operating in a continuous loop, detecting and analyzing call activity and performing threat assessments while simultaneously performing appropriate actions, tracking functions, and responses in accordance with the rules in the security policy 202.

[0087] Referring to Figure 4A, in steps 402 and 404, the process of system installation and hardware configuration, and the process of line map discovery and configuration are performed. Step 406 refers to building speech, fax and modem keyword libraries and configuring the keyword groups 308. Step 408 refers to building the codec pattern library and configuring the codec groups 312. In step 409, the PIN code groups are configured. In step 410, the extension/IP address (i.e., identifier) groups 314 are configured. Step 412 refers to security rule base 302 configuration. Step 414 refers to response policy 304 configuration. It is understood that the system administrator may perform steps 406-414 to configure the security policy 202 and the line sensor 20 from the remote management server 22, and download the configurations to one or more line sensors 20. Alternatively, the system administrator may interact directly with the one selected line sensor 20 via a terminal or terminal emulator connected to a serial port on the line sensor 20 or via a Telnet connection over the network. The line sensor 20 may be configured to allow direct administrator interaction via: (1) the serial port connection only; (2) the serial port and the remote management server 22 only; or (3) the serial port, remote management server 22, and Telnet.

[0088] In step 415, the report policy is configured, thereby formatting and designating report criteria, generation and delivery parameters for the post-event reports

218 and the schedule-generated reports 220. In step 416, the security policy 202, line  
sensor 20 configurations, keyword and pattern libraries, modifications to each, and  
software upgrades are synchronously downloaded from the remote management server 22  
to one or more line sensors 20, which are designated to receive the same groups, security  
5 policy, configurations, etc., in one or more locations within the enterprise. Conversely,  
any number of individually distinct groups, security policies, configurations, and  
modifications may be downloaded to designated line sensors 20 from the remote  
management server 22 or programmed and modified directly at the line sensor 20.

[0089] Referring now to Figure 4B, the process of call detecting and analyzing  
10 call activity begins in step 418. For each end-user station 16 and 18, and each packet-  
switched network element connected through the line sensor 20, the line sensor 20  
captures and analyzes call activity, then consolidates and reports details of the activity for  
further processing.

[0090] An aspect of this process involves the ability of the line sensor 20 to  
15 distinguish voice, fax, modem, STU-III-voice, STU-III-data, STU-III-unspecified,  
wideband data, wideband video, video, IP phone, FNBDT, TTY/TDD, busy, unanswered,  
and undetermined call types. Call type determination on a circuit-switched call is  
performed by the line sensor 20 using the received media data stream. The line sensor 20  
receives the media stream and either converts it to a linear PCM format or leaves it in a  
20 compressed format. The actual call type determination algorithm processes either the  
linear PCM data or the compressed data directly.

[0091] Having collected the media stream, the line sensor 20 processes the digital  
signal to determine the frequency domain and time domain components of the signal.

The line sensor 20 detects tone sequences, demodulates signaling handshakes, decodes message streams, and otherwise characterizes the signal contents. Based on these inputs, the line sensor 20 determines the call type.

[0092] Further analysis of call activity involves the ability of the line sensor 20 to discriminate codecs, and to detect keywords in call content via speech recognition or demodulated modem/fax data. Because the system 10 operates in a continuous processing loop, analyzing call activity while simultaneously performing appropriate actions and responses, change in call attributes during a call (e.g., call type, digits entered after call connection, codec, transmission rate, latency, jitter, etc.) are also detected.

[0093] In step 420, call attributes are compared to the rules in the security rule base 302, and pursuant to the security rule base 302, a determination is made whether to allow or deny the call. As previously described, the security rule base 302 is configured to meet the security needs of the enterprise, which may include allowing the call, in which case execution proceeds directly to step 422, denying the call, in which case execution proceeds to step 424 to cause the call to be terminated, or performing other actions including: adjusting the security policy; recording call content; redirecting the call to another end-user station 16, 18, or designated peripheral device 228; and conducting the call in encrypted mode; in which case execution proceeds to step 426. It is understood that the system administrator may manually perform preemptive or complementary actions including those described above, at any time, either at the line sensor 20 or from the remote management server 22.

[0094] In step 422, a determination is made whether the security rule base 302 designates tracking functions to be performed. If so, in step 428, the remote management

server 22 performs tracking functions, such as event logging, generating email, pager, console messaging and/or SNMP notifications, and/or generating designated reports.

[0095] In step 430, a determination is made whether the security rule base 302 designates performance of a threat assessment (action), including for example:  
5 monitoring call content for keywords; monitoring the call for the presence of patterns of interest; monitoring the call for the presence of data of interest; and initiating an authentication for remote access, as shown in step 434. If so, execution proceeds to Figure 4C and step 432, in which a TA request 328, containing all necessary information to execute the assessment, is sent to the specific system module or component that  
10 performs the designated threat assessment. In step 434, the module or component executes the designated threat assessment, such as detecting and identifying designated keywords in call content. The assessing module or component sends the result of the assessment, the TA result 330, in step 436.

[0096] In step 438, the line sensor 20 compares the TA result 330 and/or the  
15 criteria of the fired security rule base 302 rule with the rules in the result response policy 304. In step 440, a determination is made, pursuant to the result response policy 304, to either: (1) deny the call, in which case execution proceeds to step 442 to cause the call to be terminated; or (2) allow the call and perform other actions including for example, adjusting the security policy, and redirecting the call to another end-user station or  
20 peripheral device 228, in which case execution proceeds to step 444; or (3) allow the call with no additional actions, in which case execution proceeds directly to step 446. In step 446, a determination is made, pursuant to the result response policy 304, whether the remote management server 22 performs tracking functions such as event logging, generating email, pager, console messaging and/or SNMP notifications, and/or generating

designated reports in step 448. Although not shown, it is understood that additional threat assessments may be designated in step 444, in which case execution returns to step 430-436. If the process returns to step 430-436, actions and responses are performed based upon the latest TA result 330 in step 438.

5           [0097] The processes used by the line sensor 20 to detect and analyze call activity, and determine call attributes of calls on circuit-switched networks is discussed and illustrated in greater detail in U.S. Patent Application Serial No. 09/907,089 entitled TELEPHONY SECURITY SYSTEM. Also under microprocessor control, the line sensor 20 analyzes real-time packet-switched call and call information to determine call  
10 attributes for use implementing the security policy 202. The line sensor 20 uses protocol decoding and if required, decryption. The protocol packets are inspected in a stateless and/or stateful system to provide voice application security for any underlying transport such as H.323, Session Initiation Protocol (SIP), Media Gateway Control Protocol (MGCP), Media Gateway Protocol (Megaco), and proprietary protocols. Protocol packets  
15 are passed unchanged, rewritten, and/or encrypted as required by network topology or the security policy 202. Attributes are determined from the protocol packets including but not limited to source, destination, call type, codec, etc.

          [0098] Media (payload) packets are decoded and if required, decrypted. The data from the media packet is analyzed as required by the security policy 202, which may  
20 include any or all of demodulation, tone detection, speech recognition, keyword detection, and software virus/worm detection, to monitor media packets for call content. This call content can be compared with the content type determined in the protocol and policy. Media packets are passed unchanged, rewritten, and/or encrypted as required by network topology or the security policy 202. The line sensor 20 uses any or all of a range



of means to enforce the security policy 202. It can block protocol packets, block media packets, generate protocol packets, and generate media packets.

[0099] To enforce the security policy 202 and provide visibility, call activity logging, and reporting on at least all inbound and outbound real-time packet-switched calls, the basic components of the line sensor 20 includes: (1) a network or line interface; (2) a protocol processor; (3) a call data processor; (4) a security policy processor; (5) data logging memory; and (6) an administration interface. However, it will be understood by one skilled in the art that the system components listed above represent only one logical way to subdivide the functions of the line sensor 20. The functions may be subdivided into many more components or even fewer components.

[0100] The network interface physically and electrically connects the line sensor 20 to the network, recovers the digital signal from the network, and passes the digital data to the protocol processor. The network interface also receives data from the protocol processor and transmits the data onto the network.

[0101] The protocol processor inspects the data from the network interface and identifies messages. It may also inspect the messages and locate the messages that make up a real-time packet-switched connection. The protocol processor may also remove the call data from the message and pass it to the call data processor. The protocol processor also passes the call control data including source, destination, call type, compression format, etc. to the security policy processor. Finally, depending upon the results from the security policy processor, the protocol processor may send the call data back to the network interface for retransmission. Alternatively, the protocol processor may send a

message to terminate the call or may modify the contents of the call data before retransmission.

[0102] The call data processor inspects the data from the protocol processor and may decompress the data, demodulate the data, perform tone detection, perform call type  
5 discrimination, or other data analysis. The call data processor reports the results of these tasks to the security policy processor. The call data processor may also generate call data that may be used by the policy processor to generate a new call or modify an existing call.

[0103] The security policy processor inspects the call control data and the results from the call data processor. It then compares these determined attributes with the  
10 security policy 202 and determines if the call matches a rule. Pursuant to the policy, the security policy processor may command the protocol processor to retransmit the call without modification, or the security policy processor may command the protocol processor to terminate the call, modify the call data, send a message to a user, or perform some other action. Pursuant to the security policy 202, the security policy processor may  
15 also log the call, record the call data, or generate an alert.

[0104] The administration interface provides a means for the user to view and edit the security policy, generate reports that summarize call activity, review error logs and diagnostics, and configure the line sensor parameters. The administration interface transmits the security policy 202 and other configuration parameters to the security policy  
20 processor and other system components. It also receives data status and log data from the other system components for summary and display to the user.

[0105] In one embodiment, the administration interface of the line sensor 20 is an application running on the data network. In this embodiment, the administration interface

may be physically remote from the rest of the system 10. The administration interface may also be designed to provide administration for many line sensors 20 and can remotely consolidate all activity and data from many line sensors 20 into a single summary for the administrator. Likewise, the administration interface can uniformly  
5 distribute security policies 202 to all line sensors 20 or any subset thereof.

[0106] The inventive functions performed by the present invention may be implemented with commercially available components as will be understood by those skilled in the art. Although not shown, it is understood that the line sensor 20 is controlled by computer programming instructions stored in memory within the line sensor  
10 20 and which may also be stored in memory within other components of the system 10 connected to the line sensor 20.

[0107] It is understood that the present invention can take many forms and embodiments. The embodiments shown herein are intended to illustrate rather than to limit the invention, it being appreciated that variations may be made without departing  
15 from the spirit of the scope of the invention. For example, any number of different rule criteria for the security policy 202 may be defined. Different attribute descriptions and rule descriptions are contemplated. The algorithms and process functions performed by the system 10 may be organized into any number of different modules or computer programs for operation on one or more processors or workstations within the system 10.  
20 Different configurations of computers and processors for the system 10 are contemplated. The programs used to implement the methods and processes of the system may be implemented in any appropriate programming language and run in cooperation with any hardware device. The system may be used for enterprises as small as a private home or business with just a few phone lines as well as for large enterprises with multiple PBX

locations around the world, interconnected in one or more private networks or virtual private networks.

[0108] Multiple configurations are contemplated, including those wherein some or all of the functions of the remote management server 22 may be inserted into the system 10 at the line sensor 20. In an alternate embodiment, the functions of the line sensor 20 and the remote management server 22 may be inserted into the system 10 at a management line sensor (not shown) which performs some or all management server functions for all associated line sensors 20, in addition to performing all monitoring and/or controlling functions of a typical line sensor 20.

[0109] In an alternate embodiment, the management line sensor is dedicated to providing the management server functions and operations for all associated line sensors 20, and will not perform the typical monitoring and/or controlling functions of the other line sensors 20. Embodiments are contemplated wherein any of the operations and features described within this document with reference to the line sensor 20 and the remote management server 22, and their associated hardware and software components, may be implemented without a corresponding use of other operations, features and components. It is also contemplated that the line sensor 20 will process both real-time packet-switched traffic and traffic that is not real-time packet-switched traffic.

[0110] The line sensor 20 may be installed in many different locations within the circuit-switched network and/or the packet-switched network. The components of the line sensor 20 may all reside within the same device, or they may be distributed. Each of the components may consist of computer software components or electronic hardware components, or a combination of software and hardware.

[0111] As with the administration interface, the other line sensor 20 components may be physically remote from each other. In these cases, the remote line sensor component may perform its function for many line sensors 20.

[0112] The line sensor 20 may be collocated or integrated into any number of existing packet-switched network elements, including the media gateway 44, the IP firewall 56, the IP telephone 46, a gateway router, a CSU, a network hub, a network router, a bridged router, or other network device. The line sensor 20 may also be collocated or integrated into circuit-switched network elements, such as the PBX 28. If the line sensor 20 is integrated with another packet-switched network component such as a media gateway or IP Telephone, the administration interface can also provide distributed visibility and control of the functions and configuration parameters of the integrated component.

[0113] Although illustrative embodiments of the invention have been shown and described, a wide range of modification, change and substitution is intended in the foregoing disclosure and in some instances some features of the present invention may be employed without a corresponding use of the other features. Accordingly, it is appropriate that the appended claims be construed broadly and in a manner consistent with the scope of the invention.

[0114] While the present system and method has been disclosed according to the preferred embodiment of the invention, those of ordinary skill in the art will understand that other embodiments have also been enabled. Such other embodiments shall fall within the scope and meaning of the appended claims.